Technical Report

On-Demand Virus Scanning for Clustered Data ONTAP

Deployment Guide

Dhaval M Bhadeshiya, NetApp

February 2013 | TR-4127

Abstract

The On-Demand Virus Scanning solution protects corporate data hosted on the NetApp® clustered Data ONTAP® architecture from computer viruses. This solution is designed to detect and prevent the spread of malicious virus code before data is compromised. On-Demand Virus Scanning can be used to periodically scan files hosted on the clustered Data ONTAP system.

TABLE OF CONTENTS

1 Introduction

The On-Demand Virus Scanning solution protects corporate data hosted on clustered Data ONTAP from computer viruses. This solution is designed to detect and prevent the spread of malicious virus code before data is compromised. On-Demand Virus Scanning can be used to periodically scan files hosted on clustered ONTAP.

This report describes an overview of On-Demand Virus Scanning for NetApp and the best practices for deploying this solution.

1.1 Overview of On-Demand Virus Scanning for Clustered Data ONTAP

On-Demand Scanning for network drives provides protection against viruses. The AV scanning engine from AV vendors runs on Windows® Servers. Volume from the NetApp storage controller is mounted as a network drive on the Windows Server operating system and is scanned by using On-Demand Scanning.

On-Demand Scanning scans CIFS file access for threats. The AV scan engine runs on the Windows Server on which the CIFS volumes will be mounted as a network drive.

Here are some of the benefits of using On-Demand Scanning.

- **Simple implementation.** No additional infrastructure is required; existing 7-Mode Vscan farms or Windows Servers running an End-Point AV engine can be used.
- **Scheduled scanning.** Virus scanning can be performed during off-peak hours by using the On-Demand Scanning feature and scheduling scan time. The scanning options are a centralized configuration of AV from the console and the UI.

2 On-Demand Virus Scanning for the Clustered Data ONTAP Architecture

On-Demand Virus Scanning is a simple way to protect corporate data from viruses. It does not have any specific requirement for infrastructure; you can use the existing Windows Servers installed with End-Point AV engines to scan the files residing on the NetApp storage. Existing customers using a 7-Mode AV solution can continue using their AV servers to scan files on the clustered Data ONTAP system by mounting the volumes to the scan server.

3 Implementing On-Demand Virus Scanning

1. Install a Windows Server® operating system on a machine.
2. Install the End-Point AV scan engine on this server.
3. Map a network drive from the NetApp storage controller to this machine.
4. Logged-in users should have “change” permission on the file share.
5. To change permissions, go to the NetApp controller and provide “change” permission to the user who will be logged on the AV server for scanning the file share.
6. Open the AV scanning console and select On-Demand Scan.
7. Select the network drive as a scanning destination.
8. Select the remedy actions you require based on the AV provider options.

Note: For more permission-related queries, contact your antivirus vendor, because requirements may vary for different versions of scan engines from different vendors.

4 On-Demand Scanning

You can use On-Demand Scanning to perform virus scans on a schedule based on your requirements. The On-Demand Scanning commands are created by the user and can be used to scan one file or the entire cluster file system as required. The commands can be run manually or on a schedule. On-Demand Scanning generates a report upon completion.

1. The procedure for performing On-Demand Scanning is as follows: Go to the Virus scanning console > click task > New On-Demand scan task.
2. Name the task “Network Drive” and add the network drive for scanning. Alternatively, you can select all of the network drives for scanning.
3. From the Reports tab you can view the scan report after the scan is completed.
4. You can also schedule the scan based on your requirements.

Note: These steps may vary based on the antivirus vendor.

5 Remedy Options

When a file is found to be infected with a virus during scanning, the remedy option determines the course of action to take. The remedy action can be one of the following:

- Prompt for action
- Continue scanning
- Delete
- Clean

Note: Additional remedy actions may be available depending on the antivirus vendor offerings.

6 Best Practices for Antivirus Scanning

- Set up On-Demand Scanning to scan files regularly during off-peak hours or weekends using the AV engine console.
- To maximize protection, set up automatic antivirus updates.
- To maximize performance, select “Scan only executable files.” Make sure that the logged-in user account has the minimum “change” permission on the share.
- Use a multicore processor with additional RAM for better performance.
- Segregate the dataset by mapping a drive to the AV scanner under any volume on Data ONTAP.
- Consider a dedicated, direct connection to the controller for better network access.
- Use several scanners with AV installed to map different volumes/folders to decrease the overall scanning time and to be able to scan folders in parallel.

For more information about tunable parameters, contact the antivirus vendors.

7 Summary

This report collates the steps required for configuring periodic scanning for the file share residing on the NetApp controller using the End-Point antivirus scanning engine running on a Windows Server. This will help administrators to understand the configuration, architecture, and best practices for using this solution.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

Go further, faster®

NetApp®

www.netapp.com